This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for implementing a trusted counter in a personal communication device, comprising:

a secure module in a personal communication device comprising a first read-only, tamper resistant storage device, said personal communication device containing no writable storage;

a second read-write, tamper resistant storage device in an electronic card removable from the personal communication device;

a third read-write, insecure storage device in the removable electronic card; and

a processor in communication with the secure module, the second and the third storage devices configured to:

execute authentication of the second storage device by the secure module;

issue a create counter request by the secure module to the second storage device;

send a unique ID identifying a current counter value from the second storage device to the secure module;

compute an encrypted envelope of the unique ID with the secured module by applying a cryptographic transform to the unique ID; and

write a state value and the encrypted envelope of the unique ID to the third storage device.

2. (Original) The system of claim 1, wherein said state information and counter value includes the number of failed attempts to correctly enter a PIN to gain access said personal communication device.

3. (Canceled)

4. (Original) The system of claim 1, wherein said second storage device and said third storage device are external, read-write memory devices.

5. (Canceled)

6. (Original) The system of claim 3, wherein said second storage device and said third storage devices are removable electronic card that is received by said personal communication device.

7. (Original) The system of claim 1, wherein the communication between said processor and said secure module, second storage device and third storage device comprises the execution of a plurality of protocols using an operating system of the personal communication device.

8. (Original) The system of claim 7, wherein said plurality of protocols are comprised of a create protocol, a read protocol, an update protocol.

9.- 10. (Canceled)

11. (Original) The system of claim 1, wherein said personal communication device comprises a cellular telephone, a satellite telephone, a personal digital assistant or a bluetooth device.

12. (Currently Amended) The method for implementing a trusted counter in a personal communication device, comprising a first, internal read-only, tamper resistant storage device within a secure module, said personal communication device containing no writable storage , a second, external read-write, tamper resistant storage device, and a third, external read-write, insecure storage device, the method comprising:

authenticating the second storage device;

issuing a create counter request by the secure module to the second storage device;

sending a unique ID identifying a current counter value from the second storage device to the secure module;

computing an encrypted envelope of the unique ID with the secured module by applying a cryptographic transform to the unique ID; and

writing a state value and the encrypted envelope of the unique ID to the third storage device.

13. (Original) The method of claim 12, wherein said state information and counter value includes the number of failed attempts to correctly enter a PIN to access said personal communication device.

14-18 (Canceled)

19. (Original) The method of claim 12, wherein the personal communication device is a cellular telephone, a satellite telephone, a personal digital assistant or a bluetooth device.

20. (Currently Amended) A computer program product for implementing a trusted counter in a personal communication device comprising a first, internal read-only, tamper resistant storage device within a secure module, said personal communication device containing no writable storage, a second, external read-write, tamper resistant storage device, and a third, external read-write, insecure storage device, the method comprising:

a computer readable medium;

program code in said computer readable medium for authenticating second storage device;

program code in said computer readable medium for issuing a create counter request by the secure module to the second storage device;

program code in said computer readable medium for sending a unique ID identifying a current counter value from the second storage device to the secure module;

program code in said computer readable medium for computing an encrypted envelope of the unique ID with the secured module by applying a cryptographic transform to the unique ID; and

program code in said computer readable medium for writing a state value and the encrypted envelope of the unique ID to the third storage device.

21. (Original) The computer program product of claim 20, wherein the program code for authenticating of said second storage device further comprises:

program code for receiving a compliance certificate and a public key from the second storage device; and

program code for verifying the authenticity of the compliance certificate.

22. (Original) The computer program product of claim 20, wherein the program code further comprises program code for receiving a success or failure indication from said third storage device.